The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
06/15/2011

SUBJECT:
Multiple Vulnerabilities in Adobe Shockwave Player Could Allow For Remote Code Execution (APSB11-17)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Shockwave, which could allow an attacker to take complete control of an affected system. Adobe Shockwave is a multimedia platform used to add animation and interactivity to web pages. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page or when a user opens a specially crafted file. Successful exploitationwill result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts withfull user rights. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:
Shockwave Player 11.5.9.620 and earlier versions for Windows and Macintosh.

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: **High**

DESCRIPTION:
Adobe Shockwave Player is prone to multiple vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:

- Multiple memory corruption vulnerabilities in the Dirapi.dll component that could lead to code execution
- Multiple integer overflow vulnerabilities in the Dirapi.dll component that could lead to code execution
- A buffer overflow vulnerability in the Dirapix.dll component that could lead to code execution
- Multiple memory corruption vulnerabilities in the IML32.dll component that could lead to code execution
- Multiple buffer overflow vulnerabilities in the IML32.dll component that could lead to code execution

- Multiple buffer overflow vulnerabilities in the Shockwave3DAsset component that could lead to code execution
- An integer overflow vulnerability in the Shockwave 3D Asset x32 component that could lead to code execution
- An input validation vulnerability in the FLV ASSET Xtra component that could lead to code execution
- An integer overflow vulnerability in the CursorAsset x32 component that could lead to code execution
- Multiple memory corruption vulnerabilities that could lead to code execution
- An integer overflow vulnerability that could lead to code execution
- A buffer overflow vulnerability that could lead to code execution
- A design flaw that could lead to code execution

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts withfull user rights. Failed exploit attempts will likely crash the affected application.

RECOMMENDATIONS:

The following actions should be taken:

- Install the update from Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:
Adobe:

http://www.adobe.com/support/security/bulletins/apsb11-17.html

SecurityFocus:

http://www.securityfocus.com/bid/48270
http://www.securityfocus.com/bid/48278

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0317
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0318
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0319
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0320
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0335
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2108
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2109
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2111

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2112
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2113
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2114
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2115
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2116
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2117
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2118
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2119
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2120
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2121
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2122
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2123
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2124
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2125
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2126
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2127
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2128